CLAIMS

What is claimed is:

1. A method for provisioning, through a first client, a rendezvous to a user account in a server to ensure secure access to the user account by a second client through the rendezvous having an address identifier in the server, the method comprising:

establishing a communication session by the first client with the server using a first communication protocol according to the address identifier of the rendezvous; the first client having a client identification associated with the user account and running a first browser;

authenticating mutually between the first client and the server so that the communication session becomes authenticated between the first client and the server;

establishing user credential information for the rendezvous by the first client; and

associating the user credential information with the rendezvous to the user account in the server wherein the user account in the server becomes accessible by the second client through the rendezvous by supplying the user credential information thereof.

2. The method as recited in claim 1, wherein the authenticating mutually between the first client and the server comprises:

determining by the server if the first client has the user account created therefor and authorized therein according to the client identification of the first client;

sending a reply response by the server to the first client if the above determining the first client by the server succeeds, wherein the reply response comprises server information;

determining, upon receiving the reply response from the server, by the first client if the server is recognized by examining the received server information.

3. The method as recited in claim 1, wherein the authenticating mutually between the first client and the server comprises generating a session credential information comprising a mutually accepted cipher and a mutually accepted encrypt key such that all subsequent transactions between the first client and the server are encrypted by the encrypt key according to the cipher.

4. The method as recited in claim 3, further comprising:

establishing a connection by the second client to the rendezvous using a second communication protocol according to the address identifier thereof, wherein the second client runs a second browser;

supplying the user credential information to the rendezvous by the second client using the second browser;

verifying the supplied user credential information in the server; and

allowing access by the second client using the second communication protocol to the user account in the server if the supplied user credential information is verified.

5. A system for secure access over a data network to a user account, through a rendezvous identified by an address identifier, in a server, the rendezvous being exclusively designated to the user account, the system comprising:

a server coupled to the data network;

a first client, remotely located with respect to the server and coupled to the data network using a first communication protocol, having a client identification and running a first browser;

a second client, coupled to the data network using a second communication protocol, running a second browser;

a communication protocol mapper for mapping the first communication protocol to the second communication protocol and the second communication protocol to the first communication protocol, and

means for establishing an authenticated communication session between the first client and the server through the data network, the authenticated communication session establishing means comprising:

means for recognizing the first client by the server according to the client identification and

means for recognizing the server by the first client according to a reply response from the server after the first client is recognized by the server.

6. The system as recited in claim 5, further comprising means, in the first client and through the established authenticated communication session, for updating the rendezvous with user credential information.

7. The system as recited in claim 6, further comprising means for verifying the user credential information supplied by the second client using the second browser after the second client logs onto the rendezvous according to the address identifier thereof.

8. The system as recited in claim 7 wherein the first client is a thin computing device and wherein the first browser is a micro-browser.

9. The system as recited in claim 7 wherein the first client is a mobile phone; wherein the first browser is an Handheld Markup Language browser and wherein the first communication protocol is Handheld Device Transport Protocol.

10. The system as recited in claim 9 wherein the second client is a personal computer coupled to the data network.

11. The system as recited in claim 10, wherein the second communication protocol is Hypertext Transfer Protocol and wherein the second browser is an Hypertext Markup Language browser.

12. A method for provisioning, through a first client, a rendezvous to a user account in a server to ensure secure access to the user account by a second client through the rendezvous having an address identifier in the server, the method comprising:

initiating a transaction signal by the first client to the server using a first communication protocol; the first client having a client identification associated with the user account and running a first browser, wherein the transaction signal comprises the client identification and the address identifier of the rendezvous;

examining a communication session between the first client and the server, wherein the examining session comprises:

creating the communication session between the first client and the server if the communication session is not in existence or is not valid;

conducting mutual authentication between the first client and the server; and

generating session credential information for the communication session such that subsequent transactions are encrypted by the session credential information;

establishing by the first client user credential information for the rendezvous if the communication session is valid; and

associating the user credential information with the rendezvous to the user account in the server.

13. The method as recited in claim 12 further comprising updating the managed information in the user account in the server by the first client using the first browser.

14. The method as recited in claim 13, wherein the first browser is a micro-browser.

15. The method as recited in claim 14, wherein the first browser is an Handheld Device Markup Language browser.

16. The method as recited in claim 15 wherein the initiating the transaction signal comprises hyperlinking the rendezvous using the first communication protocol according to the address identifier of the rendezvous.

17. The method as recited in claim 16 wherein the first browser is Handheld Device Markup Language browser and wherein the first communication protocol is Handheld Device Transfer Protocol.

18. The method as recited in claim 17, wherein the user credential information comprises a username and a password;

19. The method as recited in claim 12, wherein the transaction signal initiated by the first client comprises the address identifier of the rendezvous.

20. The method as recited in claim 19, wherein the mutual authentication conducting between the first client and the server comprises the server conducting a client authentication and the client conducting a server authentication, wherein the client and the server are communicated in the authenticated communication session.

21. The method as recited in claim 12, wherein the transaction signal initiated by the first client comprises at least one client message encrypted by a secret encrypt key shared between the first client and the server.

22. The method as recited in claim 21, wherein the mutual authentication conducting between the first client and the server comprises:

conducting a first client authentication in the server by decrypting the encrypted client message in the transaction signal from the first client;

conducting a first server authentication in the first client by decrypting an encrypted server message in a server response from the server after the first client authentication in

the server succeeds, wherein the server response further comprises a session key and a client derivative of the client message;

conducting a second server authentication in the first client by verifying the client derivative with respect to the client message;

conducting a second client authentication in the server by decrypting a client response from the first client wherein the client response comprises a server derivative of the server message; and

finalizing session credential information comprising a session ID, the session key and a mutually agreed cipher such that subsequent transactions between the first client and the server are encrypted by the session key according to the mutually agreed cipher.

23. The method as recited in claim 12 further comprising:

establishing a second communication session between the second client and the server using a second communication protocol according to the address identifier of the rendezvous;

providing the user credential information, by the second client, to the rendezvous;

verifying the user credential information provided by the second client in the server; and

accessing the managed information in the user account in the server by the second client using a second browser if the user credential information supplied by the second client is verified.

24. The method as recited in claim 23, wherein the establishing the communication session between the second client and the server comprises creating the communication session between the second client and the server if the communication session is not in existence or is not valid.

25. A system for secure access, through a rendezvous having an address identifier, a user account in a server, the rendezvous being exclusively designated to the user account, the system comprising:

a data network comprising an airnet supporting a first communication protocol and a landnet supporting a second communication protocol, the landnet coupled to the server;

a first client, remotely located with respect to the server and coupled to the airnet using a first communication protocol, having a client identification exclusively associated with the rendezvous and running a first browser ;

a second client coupled to the landnet using a second communication protocol and running a second browser;

means for mapping the first communication protocol to the second communication protocol and the second communication protocol to the first communication protocol; the first client communicating with the server via the communication protocol means;

means for creating an authenticated and secure communication session between the first client and the server through the data network; the session creating means comprising:

means for requesting the session by the first client to the server if the session is not in existence or in not valid;

means for conducting mutual authentication between the first client and the server; and

means for generating session credential information for the session in creation;

means, in the first client and through the created session, for updating the rendezvous with user credential information by a first browser such that the user account is accessible by the second client through the rendezvous with the user credential information.

26. The system as recited in claim 25, further comprising means, in the second client, for providing the user credential information to the rendezvous so as to access the user account in the server, thereby the second client can update the managed information therein using the second browser.

27. The system as recited in claim 26 wherein the first client is a mobile computing device and wherein the first browser is a micro-browser.

28. The system as recited in claim 27, wherein the first client is a cellular telephone and wherein the first communication protocol is Handheld Device Transfer Protocol and wherein the first browser is Handheld Device Markup Language.

29. The system as recited in claim 27, wherein the first client is a cellular telephone and wherein the first communication protocol is Hypertext Transfer Protocol and wherein the first browser is Handheld Device Markup Language browser.

30. The system as recited in claim 25, wherein the conducting mutual authentication means comprises:

means for conducting first client authentication in the server;

means for conducting first server authentication in the first after the first client authentication in the server succeeds;

means for conducting second server authentication in the first client; and

means for conducting second client authentication in the server after the first and second server authentication succeed in the first client.

31. The system as recited in claim 30, further comprising means for generating session credential information for the first client and the server; wherein the credential information comprises a session ID, a session key and a mutually agreed cipher such that

subsequent transactions between the first client and the server are encrypted by the session key according to the mutually accepted cipher;

Ins A37